Chapter 2
Introduction

This chapter describes the features of the NETGEAR ProSafe Wireless 802.11g VPN Firewall Model FVG318.

Key Features of the Wireless VPN Firewall

The ProSafe Wireless 802.11g VPN Firewall Model FVG318 with eight-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem and provides 802.11b/g wireless LAN connectivity.

The FVG318 is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing firewalls that rely on Network Address Translation (NAT) for security, the FVG318 uses stateful packet inspection for Denial of Service attack (DoS) protection and intrusion detection. The FVG318 allows Internet access for up to 253 users. The FVG318 wireless VPN firewall provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts — both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 personal computers. In addition to NAT, the built-in firewall protects you from hackers.

With minimum setup, you can install and use the firewall within minutes.

The FVG318 wireless VPN firewall provides the following features:

- 802.11g and 802.11b standards-based wireless networking.
- *Wireless Multimedia (WMM) support.*
- Easy, Web-based setup for installation and management.
- Front panel LEDs for easy monitoring of status and activity.
- Content filtering and site blocking security.
- Built-in eight-port 10/100 Mbps switch.
- Ethernet connection to a WAN device, such as a cable modem or DSL modem.
- Extensive protocol support.
- Flash memory for firmware upgrade.

802.11g and 802.11b Wireless Networking

The FVG318 wireless VPN firewall includes an 802.11g-compliant wireless access point. The access point provides:

- 802.11b standards-based wireless networking at up to 11 Mbps.
- 802.11g wireless networking at up to 54 Mbps, which conforms to the 802.11g standard.
- WPA and WPA2 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation.
- WPA-PSK and WPA2-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA and WPA2.
- 64-bit and 128-bit WEP encryption security.
- WEP keys can be generated manually or by passphrase.
- Wireless access can be restricted by MAC Address.
- Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect.

Wireless Multimedia (WMM) Support

WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information such as video or audio will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT firewalls, the FVG318 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection.

  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents.

The FVG318 logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your e-mail address or email pager whenever a significant event occurs.

- With its content filtering feature, the FVG318 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Security

The FVG318 wireless VPN firewall is equipped with several features designed to maintain security, as described in this section.

- PCs Hidden by NAT
  NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.
- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated “DNS” host computer. You can specify forwarding of single ports or ranges of ports.

Autosensing Ethernet Connections with Auto Uplink

With its internal eight-port 10/100 switch, the FVG318 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The firewall incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a normal connection such as to a PC or an uplink connection such as to a switch or hub. That port then configures itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The FVG318 wireless VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to “Internet Networking and TCP/IP Addressing:” in Appendix A.”

- IP Address Sharing by NAT
  The FVG318 wireless VPN firewall allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP
  The FVG318 wireless VPN firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- Point-to-Point Protocol over Ethernet (PPPoE)
  PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as Entersys or WinPOET on your PC.

Easy Installation and Management

You can install, configure, and operate the ProSafe Wireless 802.11g VPN Firewall Model FVG318 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management
  Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided, and online help documentation is built into the browser-based Web Management Interface.
- Smart Wizard
  The FVG318 wireless VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- Diagnostic functions
  The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot.

- Remote management
  The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- Visual monitoring
  The FVG318 wireless VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the FVG318 wireless VPN firewall:

- Flash memory for firmware upgrade.
- Free technical support seven days a week, 24 hours a day.

Package Contents

The product package should contain the following items:

- ProSafe Wireless 802.11g VPN Firewall Model FVG318.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- Installation Guide.
- *Resource CD*, including:
  - This guide.
  - Application Notes and other helpful information.
- Registration and Warranty Card.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the firewall for repair.

The FVG318 Front Panel

The front panel of the FVG318 wireless VPN firewall contains the status LEDs described below.

Figure 2-1

You can use some of the LEDs to verify connections. Viewed from left to right, Table 2-1 describes the LEDs on the front panel of the firewall. These LEDs are green when lit.

Table 2-1. LED Descriptions

LED Label	Activity	Description
PWR	On	Power is supplied to the firewall.
TEST	On Off	The system is initializing. The system is ready and running.
INTERNET		
100 (100 Mbps)	On Off	The Internet (WAN) port is operating at 100 Mbps. The Internet (WAN) port is operating at 10 Mbps.
LINK/ACT (Link/Activity)	On Blinking	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
LOCAL		
100 (100 Mbps)	On Off	The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps.
LINK/ACT (Link/Activity)	On Blinking	The Local port has detected a link with an attached device. Data is being transmitted or received by the Local port.
WLAN	On/Blink Off	The wireless interface is on/data transmission in progress. The wireless interface is off.

The FVG318 Rear Panel

The rear panel of the FVG318 wireless VPN firewall contains the port connections listed below.

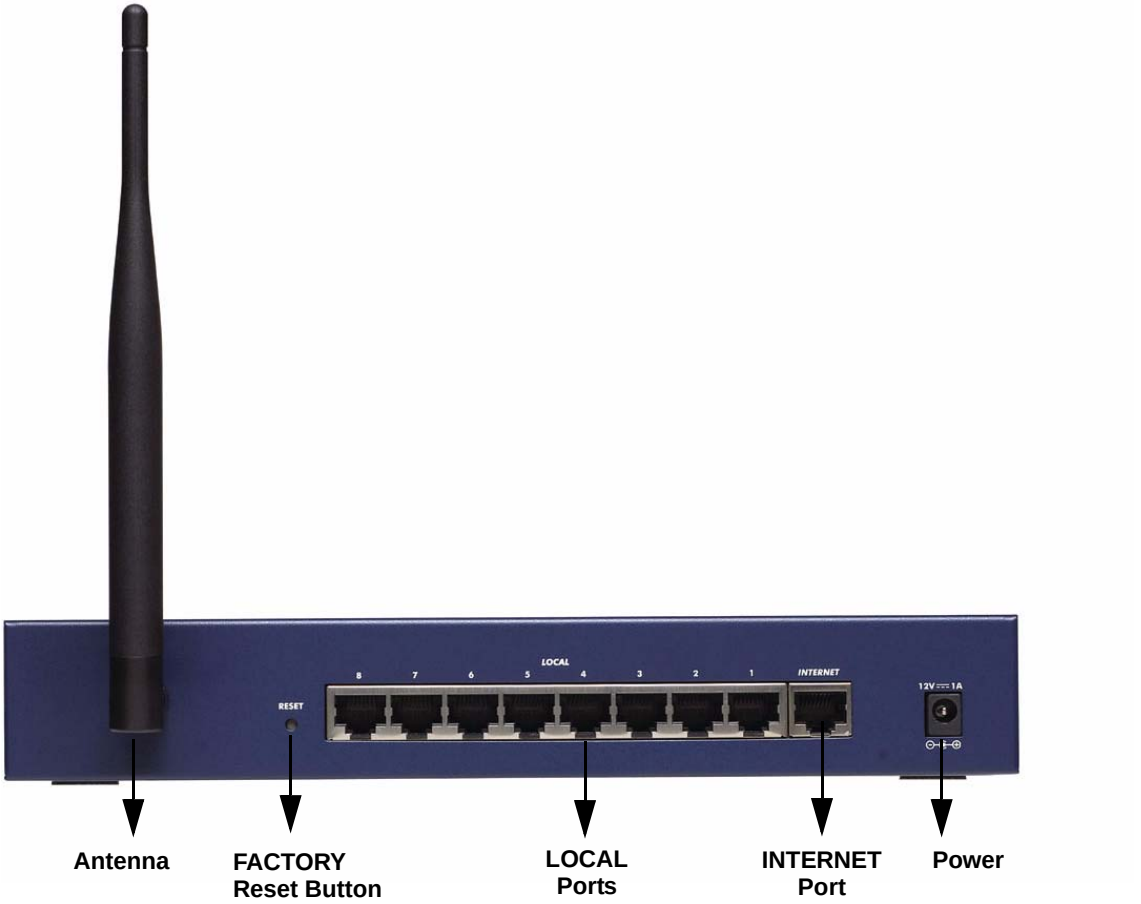

Figure 2-2

Viewed from left to right, the rear panel contains the following features:

- Detachable wireless antenna
- Factory default reset push button
- Eight Ethernet LAN ports
- Internet Ethernet WAN port for connecting the firewall to a cable or DSL modem
- DC power input

NETGEAR-Related Products

NETGEAR products related to the FVG318 are listed in the following table:

Table 2-1. NETGEAR-Related Products

Category	Wireless	Wired
Notebooks	WAG511 108 Mbps Dual Band PC Card WG511T 108 Mbps PC Card WG511 54 Mbps PC Card WG111 54 Mbps USB 2.0 Adapter MA521 802.11b PC Card MA111 802.11b USB Adapter	FA511 CardBus Adapter FA120 USB 2.0 Adapter
Desktops	WAG311 108 Mbps Dual Band PCI Adapter WG311T 108 Mbps PCI Adapter WG311 54 Mbps PCI Adapter WG111 54 Mbps USB 2.0 Adapter MA111 802.11b USB Adapter	FA311 PCI Adapter FA120 USB 2.0 Adapter
PDAs	MA701 802.11b Compact Flash Card	
Antennas and Accessories	ANT24O5 5 dBi Antenna ANT2409 Indoor/Outdoor 9 dBi Antenna ANT24D18 Indoor/Outdoor 18 dBi Antenna Antenna Cables–1.5, 3, 5, 10, and 30 m lengths VPN01L and VPN05L ProSafe VPN Client Software	

NETGEAR Product Registration, Support, and Documentation

Register your product at *http://www.NETGEAR.com/register*. Registration is required before you can use our telephone support service.

Product updates and Web support are always available by going to: *http://kbserver.netgear.com.*

Documentation is available on the Resource CD and at http://kbserver.netgear.com.

When the wireless VPN firewall is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the wireless VPN firewall.